NPS-54-90-011

NAVAL POSTGRADUATE SCHOOL

Monterey, California

PASSWORDS SECURITY:

AN EXPLORATORY STUDY

by

Moshe Zviran and William J. Haga

May 1990

Naval Postgraduate School
Monterey, California

RADM. R. W. West, Jr.
Superintendent

Harrison Shull
Provost

The research summarized herein was accomplished with funding provided by the Research Council of the Naval Postgraduate School.

This report was prepared by:

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a REPORT SECURITY CLASSIFICATION Unclassified	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S) NPS-54-90-011	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) AS(54)
6c ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School
8a NAME OF FUNDING / SPONSORING ORGANIZATION NPS Research Foundation	8b OFFICE SYMBOL (If applicable)
8c ADDRESS (City, State, and ZIP Code) Naval Postgraduate School Monterey, CA 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000
	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER O&MN, Direct Funding
	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT ACCESSION NO.

11 TITLE (Include Security Classification)
Passwords Security: An Exploratory Study (Unclassified)

12 PERSONAL AUTHOR(S)
Moshe Zviran and William J. Haga

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Technical Report	FROM _____ TO _____	May 199[illegible]	42

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Computer Security, Passwords

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

One of the most common control mechanisms for authenticating users of computer-based information systems is the use of passwords. However, despite the widespread use of passwords, only little attention has been given to the characteristics of their actual use.

This paper addresses the gap in evaluating the characteristics of real-life passwords and presents the results of an empirical study on passwords usage. It investigates the core characteristics of user-generated passwords in a DoD environment and associations between those variables.

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL Moshe Zviran	22b TELEPHONE (Include Area Code) 408-646-2[illegible]

DD Form 1473, JUN 86

Passwords Security: An Exploratory Study

By

William J. Haga and Moshe Zviran

Department of Administrative Sciences

Naval Postgraduate School

Monterey, CA. 93943

Tel: (408) 646-2489, Bitnet: 5046P@NAVPGS

May 1990

Passwords Security: An Exploratory Study

Abstract

One of the most common control mechanisms for authenticating users of computer-based information systems is the use of passwords. However, despite the widespread use of passwords, only little attention has been given to the characteristics of their actual use.

This paper addresses the gap in evaluating the characteristics of real-life passwords and presents the results of an empirical study on passwords usage. It investigates the core characteristics of user-generated passwords in a DoD environment and associations between those variables.

CR Categories and Subject Descriptors:

D.4.6 [Security and Protection]: access control; authentication.

General Terms: Computer security, passwords.

Introduction

The proliferation of computer technology has bred opportunities for ill-intentioned individuals to violate the integrity and validity of computer-based information systems. At the same time, a growing dependence on computer-based information systems creates an urgent need to collect information and render it accessible.

A fundamental access control method in any computer-based information system is the ability to authenticate the identity of a system user. While research continues on more sophisticated methods of authentication, password mechanisms remain the predominant method of authenticating users of computer-based information systems [2, 6, 9, 10, 12, 15, 18, 21, 23]. A password is a mutually agreed upon code word, assumed to be known only to the user and the operating system. In some cases a password is chosen by a user while in other cases it is generated and assigned by the security kernel of the operating system. The length and format of passwords vary from one information system to another [6, 8, 12, 18].

Passwords are known to suffer from several pitfalls. First, the tradeoff between memorability and safety poses a difficult dilemma in the generation of passwords. Passwords should be difficult to guess and easy to remember [8, 11, 18, 19, 25]. For passwords to be difficult to guess, they should be selected from a large domain. Nevertheless, if passwords are chosen to make them difficult to guess, they may also be difficult to remember. The most secure type of passwords is a random string of characters [3, 19, 24]. Although such passwords are difficult to guess by others, users generally dislike them as random, arbitrary, passwords are difficult to remember. Instead, most users will resort to meaningful details, such as name, nickname, initials,

birthdate, and so on [3, 15].

A password that is difficult to remember compels a user to write it down, ensuring they will not forget them but compromising its secrecy [17]. On the other hand, if a difficult password is not written down, it may well be forgotten, resulting in serious inconvenience [2, 19]. Therefore, an organization should establish a password policy that strikes a balance between ease of remembrance and susceptibility to compromise [24].

Despite the widespread use of passwords, only little attention has been given to the characteristics of their actual use. A unique effort to reveal the characteristics of passwords used in a real-life system was presented in 1979 by Morris and Thompson [14]. Their paper described the basic characteristics of user-generated passwords in a UNIX environment and analyzed the level of security provided by these passwords. No follow-on research or additional empirical work on password usage and characteristics have been reported ever since. This paper addresses the gap in evaluating the characteristics of real-life passwords and presents the results of an empirical study on passwords usage.

Research Method

Source of the Data

To assess password practices and experiences, questionnaires were sent to graduate students and faculty and staff members at the Naval Postgraduate School in Monterey, California.

At the Naval Postgraduate School, which is a management and engineering graduate school, both students and faculty have access to the campus computing center's

mainframe without user charges. The mainframe can only be accessed with a combination of a user-id (assigned by the computing center) and a user-generated password. Once access to the school's mainframe has been granted, a user is provided with an immediate access to a large variety of computing resources within the Department of Defense (DoD) through the DoD communications network.

This survey, however, was not limited to questions about password practices to access the campus mainframe. Users were also asked about the way they employed passwords on the school's departmental minicomputers, instructional PC networks linked to the mainframe and computer-based information systems at other institutions.

Instrumentation

The questionnaire asked for responses in four major areas: user demographics, password characteristics, password memorability and the importance and sensitivity of user data files. Appendix A contains the entire questionnaire.

Demographic items: Age, sex and organizational affiliation (department or academic curriculum).

Password characteristics: The number of characters in a password, its structure (alphabetic, numeric, alphanumeric or ASCII) and the basis for choosing a password. How a password was chosen means whether it was based on a personally meaningful detail (user's last name, first name, nick name, child's name or some other easily recalled bit of personal, biographical information), a combination of meaningful details (BILL89 or LOVEMARY), a pronounceable string of characters (2BFREE), string of random characters (H*DGFH8H) or some other basis.

Password Memorability and Computer Usage Characteristics: Difficulty in remembering a password (yes or no), if the password was written down (yes or no), and if so, where. Multiple choice options were provided for where it might be written down (wallet, notebook, calendar, desk, etc.).

Importance and Sensitivity of User Data Files: Users were asked to separately rate both the importance and the sensitivity of their data files on a scale of one to five. Data importance referred to the inherent value of the data to an individual user. Sensitivity means the degree to which problems would arise if the contents of their data files were known to others. To distinguish between importance and sensitivity of a data file, consider, for example, a data file containing the text of a student's graduate thesis might not be publicly sensitive but it would be of irredeemable value to its author. By comparison, a professor's data file containing student course grades would have little inherent value but would highly sensitive to disclosure. Indeed, divulging such a list could violate U.S. laws regarding privacy of information.

Sample Characteristics

The questionnaires were distributed to 1600 students and 400 faculty and staff members at the Naval Postgraduate School. The questionnaires were distributed through the school's internal mail system. 997 questionnaires (49.9%) were returned, of which 208 were from faculty/staff while 789 were from students. 903 of the respondents were males and 94 were females. The average age of the respondents was 34, ranging form 23 to 76. Of these, 860 (43%) used passwords and were included in the following analysis.

Findings

Number of Characters in Password

The average number of characters in a password, calculated from the password lengths in this study, was six. Figure 1 shows that passwords of five and six characters were nearly tied in popularity and 80% of the respondents used a 4-7 characters password. While the DoD recommends that passwords should be, at a minimum, six characters in length [5], 47% of the surveyed passwords failed to do so. Menkus [15] further supports this password length guideline and suggest that the ideal length is six to eight characters.

Insert Figure 1 about here

How Users Chose a Password

As Figure 2 shows, users strongly preferred (78.4%) passwords made up from a meaningful detail or a combination of meaningful details. Examples of meaningful details are names, nickname, name of child, name of pet, name of spouse or birth date. The item has meaning for the person using it which should enhance its memorability. 13.1% of the respondents did not answer this particular question.

Insert Figure 2 about here

Structure of Passwords

Figure 3 presents the structure of the surveyed passwords. 80.1% of the respondents preferred alphabetic structure for their passwords, where only 0.7% used the entire ASCII character set as a basis to constructing their password.

Insert Figure 3 about here

How Many Wrote Down Password

Only 9.7% of the users reported having difficultly in remembering their password. However, 23.3% of the respondents wrote down their password. When a user writes down a password, it is usually in an insecure location [22]. Once a password is written down it is no longer something known but becomes something possessed [19]. Searching through a user's notebook, desk, diary or users manual is a good means to discovering a password [2].

Where Password Is Written Down

The DoD Password Management Guidelines [5] recommend that "If passwords must be written, they should be protected in a manner that is consistent with the damage that could be caused by their compromise" [5, p. 8]. Figure 4 shows that, among the respondents who said they wrote down their password, the location of choice was the wallet (42.1%) followed by a notebook (21.3%).

Insert Figure 4 about here

Frequency of Changing Password

While the periodic changing of a password is a basic security measure [5, 18], Figure 5 reveals that 79.5% of these users never changed their password. Less than 5.6% of them changed passwords more of than once a year.

Insert Figure 5 about here

Relationships Between Password Characteristics

Based on these findings, an attempt has been made to relate the variables under investigation to these findings. The rationale for this analysis was to find whether password memorability and ease of guessing are associated with variables assessed by this survey. Five research questions have been addressed:

1) What variables are associated with a decision to write down a password.

2) What factors are related to how difficult a password is to remember.

3) The variables that are related to the ease of guessing a password.

4) How the sensitivity of data are related to password selection.

5) How the importance of data are related to password selection.

The null hypothesis (H_0) in all cases was that no association existed between the two items being tested. The cutoff point for rejecting a null hypothesis was a probability greater than .05 that the tested association could have happened by chance. Table 1 portrays the various statistical tests for association that have been employed. The selection of the appropriate test depends on the nature of the variables under investigation [20]. All statistical computations were made with SPSS-X [16].

Insert Table 1 about here

Writing down a password

Responses to the question "do you write down your password?" (a dichotomous response) were examined for their association with six variables. It had been assumed that users write down a password if:

1. It has a high number of characters in it (variable called "Number").
2. The characteristics of the password make it difficult to remember, e.g. random string or ASCII characters (variable called "Password").
3. It was poorly chosen (variable called "Chosen").
4. It is changed frequently (variable called "Change").
5. It is difficult to remember (variable called "Remember").
6. It is not used frequently (variable called "Log On").

Insert Table 2 about here

Table 2 shows that the assumption that users will write down a password if it has a high number of characters in it was not supported. This finding is not surprising. The number of characters in a password is expected to affect memorability. It follows that if a password is difficult to remember it is written down [2].

System-generated passwords typically consist of pseudo-random characters [15, 24]. They, therefore, tend to be complicated, difficult to remember and lack popularity with users [24]. If a password is not easy to remember then users tend to write it down [2]. 83 users found it difficult to remember their passwords. However, 200 users felt it was necessary to write down their passwords. Users who perceive that they will not be using the computer-based information system on a frequent basis may choose to write down their password for future reference. Users may write down their password simply out of habit. Or users may write down a password because frequent change requirements are too demanding for their mental capacity or desire to remember. More change increases the likelihood a password will be forgotten.

Table 2 also indicates that while there is not a strong association between writing down a password and its characteristics, it is statistically significant. The findings here demonstrate that the characteristics of a password have something to do with whether a user is moved to put it in writing. Here it was assumed that the characteristics of a password would affect its memorability which would lead to it being written down.

These findings provide no confirmation for the assumption that frequent password changing would make it difficult to remember the current password which would cause users to write down the password. The finding of a statistically significant association between difficulty remembering a password and whether it was written down supports previous research [2].

The frequency with which a password is used was found to have a statistically significant relationship to whether it is written down. This supports the assumption that little use of a password to access a computer-based information system leads to the password being forgotten. If it is not forgotten the need to write it down is reduced.

Difficulty Remembering a Password

A second issue of interest were possible relations of a user's difficulty to remember a password and a set of relevant variables. Responses to the question "do you have difficulty remembering a password ?" (a dichotomous response) were examined for their association with answers to six other questions. It had been assumed that users would have trouble remembering a password if:

1. It has a high number of characters in it (variable called "Number").
2. The characteristics of the password make it difficult to remember, e.g. random string or ASCII characters (variable called "Password").
3. It was poorly chosen (variable called "Chosen").
4. It is not used often (variable called "Log On").
5. It is changed frequently (variable called "Change").
6. It is not the same password used on other information systems (variable called "Same").

Insert Table 3 about here

Barton and Barton [3] and Menkus [15] suggest that the ability to recall a password tends to decrease as length increases. It has long been accepted that people can remember expressions of about seven characters in length [13] with a proposed password length being six to eight characters [15]. The findings shown in Table 3 do not support those suggestions.

Table 3 also contains a finding that the characteristics of a password are associated with difficulty remembering it. As previous research revealed. an alphanumeric password chosen from meaningful detail is more easily remembered than passwords generated from pseudo-random combinations [24].

There was a finding of a significant association between the basis for choosing a password and whether it is difficult to remember. Users who choose their own password are more likely to remember it [24]. Users will select from a simple domain of things meaningful to them, something from episodic memory [15, 24].

A significant and strong association was found between how often a password was used and how difficult it is to remember. This supports the assumption that frequent use of a computer-based information system is related to password memorability. Table 3 also shows a significant and strong association between frequent change of a password and how difficult it is to recall that supports previous research [22]. The frequency with which a password is changed may result from a password being difficult to remember, the suspicion that a password has been guessed or security consciousness.

Finally, no relationship was found between the use of the same password on several information systems and whether it was difficult to remember.

Predictability of a Password

Password compromises have resulted from information on computer bulletin boards, guesses about personal vitae, environmental cues and systematic intrusions [3]. The predictability of a password is expected to be influenced by password characteristics, frequency of use and whether the password was written down, how often it is changed, frequency of using the computer-based information system and the work location of the user.

Responses to the question "has your password been guessed?" (a dichotomous response) were examined for their association with answers to seven other questions. It was assumed that a password was predictable if:

1. It had been written down (variable called "Write").
2. It has a low number of characters in it (variable called "Number").
3. The characteristics of the password make it easy to guess (variable called "Password").
4. It was poorly chosen (variable called "Chosen").
5. It is used frequently (variable called "Log On").
6. It is not changed frequently (variable called "Change").
7. The user accesses the information system from a public terminal (variable called "Work").

Insert Table 4 about here

Table 4 shows that there was no significant relationship between a password having been written down and whether the password was predictable. This finding is not in standing with previous research that suggests once a password is written down it becomes something possessed that can be stolen.

Morris and Thompson [14] suggest that a shorter password means less work to do in a brute force attack to discover a user's password. While this view is widely supported in the literature (Avarne [2], Hsiao [8] and Pfleeger [18] are just a few to mention), the findings in Table 4 do not support it. Those respondents thinking that their password might have been compromised, had not associated this compromise with the length of the password.

Table 4 also shows that the characteristics of a password and its predictability, while not strongly associated, are statistically significant. The link here is that passwords chosen from a meaningful detail from the user's biography make a password predictable. This supports earlier research. Relatively short passwords chosen from some form of meaningful detail and consisting of alphanumerics increase predictability, Morris and Thompson [14] found that an intruder conducting a dictionary search alone would require only five minutes to reveal about a third of the 3,269 passwords collected.

How a password was chosen and its predictability were found not to be significantly associated. This finding contradicts previous research. Morris and Thompson [4] suggest that passwords consisting of letters and numbers were more predictable than passwords consisting of, say, than ASCII characters.

There was no association in Table 4 between the frequency with which a password was used and its predictability. The literature on password security suggests that frequent use of a password increases its predictability [1, 2].

These findings show that there was a strong association between the frequency with which a password was changed and its predictability. Most previous research supports the frequent changing of passwords to reduce predictability. Wood [24] asserts that passwords should be changed annually. Menkus [15] suggests every 30 days. While changing a password is believed to be a sound security practice for information system access it also makes it difficult for a user to remember his or her current password.

The findings here also show that where a user worked was related to the predictability of their password. A public terminal is clearly a more vulnerable work site than the privacy of a faculty office or accessing the mainframe by modem from home. 19% of the user worked at home and 16% worked from a private office. 51% worked at public terminals. Those who worked at home had the least predictable passwords.

If a user had a predictable password, they were then asked why they thought it had been compromised. 23% of the compromised users had data files that had been altered. 26% had unintentionally disclosed the password to others. 10% had intentionally disclosed a password. 39.5% attributed their belief to other indicators.

Data Importance

Data importance is an assessment of how crucial data files are. It had been assumed that data rated as important would be surrounded with more security than data not rated as crucial [7]. Responses to the question "how important are your data?" (an ordinal response) were examined for their association with answers to six other questions. It had been assumed that if data files are rated as being important then:

1. Passwords would not be written down (variable called "Write").
2. Passwords would be longer (variable called "Number").
3. The characteristics of the password would make it predictable (variable called "Password").

4. The password would be well chosen (variable called "Chosen").
5. The password would be changed frequently (variable called "Change").
6. The user would avoid accessing the information system from a public terminal (variable called "Work").

Insert Table 5 about here

As can be seen from Table 5, there were no associations between data importance and password characteristics or the number of characters in a password. This lack of association can be explained by understanding that when most users are issued a mainframe account, they have little anticipation of what kind of information they will be storing in their data files.

Table 5 shows a significant association between writing down a password and how important were a user's data files. Writing down a password, of course, invites a compromise of computer-based information system security. This finding contradicts the assumption that important data would be treated with greater care. A security-conscious user will with important data files will not write down a password for fear of it being lost. Once written down the degree of security is compromised.

There was confirmation of the assumption that users take care to choose passwords that are difficult to predict for data they consider important. These findings also provided grounds for the assumption that users undertake the precaution of frequently changing their passwords in order to protect important data.

There also was confirmation for the belief that users took care not to work from public terminals If they considered their data files to be important.
Typically, if a user is working on an important data file they will do somewhere that is more secure than a public terminal room.

Data Sensitivity

Data sensitivity refers to the degree to which embarrassment or problems would result from the disclosure of the data. As with the importance of data files, it had been assumed that as users rated their data as more sensitive, they would be more cautious in the use of the password that accessed them [7].

Responses to the question "how sensitive are your data?" (an ordinal response) were examined for their association with answers to six other questions. It had been assumed that if users rated their data files as containing sensitive information then:

1. They would not write down their passwords (variable called "Write").
2. They would use longer passwords (variable called "Number").
3. The characteristics of the password would make it predictable (variable called "Password").
4. The password would be well chosen (variable called "Chosen").
5. The password would be changed often (variable called "Change").
6. The user would avoid accessing the information system from a public terminal (variable called "Work").

A secure password is one that is relatively long, made up of random alphanumerics, is easy to remember and difficult to predict.

Insert Table 6 about here

The results in Table 6 suggest that there were no associations between data sensitivity and whether a password was written down, how a password was chosen, password characteristics or the number of characters in a password. However, Table 6 does contain a finding that the sensitivity of data files is related to how often passwords were changed. As with the importance of data files, users were making distinctions in their management of passwords to protect sensitive files. Finally, the findings here support the assumption that the sensitivity of data files is related to users' work locations. Again, as with data file importance, users took precautions in how they used their passwords, i.e. not working on sensitive data where the password access might be observed by others.

Discussion

Passwords As An Effective Access Control Mechanism

Little of the literature on password security is empirically-based. The bulk of it consists of essays offering common-sensical suggestions about how users ought to employ passwords based on widely-held assumptions about how they do employ them. The effort here looks at the empirical reality behind those assumptions.

This paper points out that access control to a computer-based information system is required at various levels in order to obtain a required level of security. At each level a certain amount of user identification, authentication and authorization must be verified. Passwords were found to be an effective means for such. Traditional passwords,

however, have some inadequacies. Morris and Thompson (1979) revealed some of the inadequacies of user-generated passwords in the pre-personal computer era. Some of these inadequacies included passwords relatively short in character length and passwords made up of some type of meaningful detail to the user making them easy to remember. Passwords that are easy to remember provide low levels of security.

This empirical verification of password practices identifies the characteristics that affect password selection, memorability and predictability. Moreover, it brings to light that the importance and sensitivity of data files affect how password selection, memorability and predictability.

From the descriptive findings, two stand out. Despite long efforts by information system professionals to inculcate users with proper password practices, this study found that users continue to choose short passwords made up mostly of easy-to-remember alphanumeric characters.

Characteristics of User-Generated Passwords

This paper has shown that the characteristics of user-generated passwords in the personal computer era have not changed much from those characteristics in the pre-personal computer era identified by Morris and Thompson [14]. User-generated passwords of today still bear the characteristics of being made up of some type of meaningful detail to the user, relatively short in length, made of alphabetic or alphanumeric characters and, in some cases, written down on paper. In general, they remain easy to remember and simple in structure. However, what has changed is the user's attitude toward security on computer-based information systems. The impetus of computer security has made the common user more privy to computer security

requirements and more receptive to organizational administrative and technical security controls/procedures.

Password Characteristics And Writing Down A Password

Most users require memory aids to help their recall [15]. The most common type of memory aid is writing a password down. This violates the basic tenet of password security. Typically, a password is written down if it is difficult to remember [2]. However, passwords are also written down out of habit, from the perception that the password will not be used frequently or because system change requirements are too demanding to remember each password. This research showed that password memorability affects whether a password is written down.

The analysis of the relationships among the password variables produced both confirmations of some pieces of the conventional wisdom in regard to system security as well as some surprises.

Among the confirmations were these:

1. If a password was difficult to recall it was written down.
2. The more frequent a password was used, the less it was written down.
3. The more a password is used, the less difficult it is to remember.

Among the surprises were the following:

1. The length of passwords is not related to their being written down.
2. Whether a password was chosen on a basis that helped its memorability or impeded it had no bearing on its being written down.

3. The length of passwords is not related to whether they are difficult to recall.
4. Frequent changing of passwords, necessary to reduce password predictability, nonetheless hinders recall.
5. The number of characters in a password is not related to its predictability.
6. There was no support for the commonplace that alphanumeric characters make a password more predictable than ASCII characters.

Many of the notable findings reported here are neither confirmations nor surprises because they introduce dimensions of password security heretofore not explored in the literature, e.g. data file importance, data file sensitivity and work location,

Password Characteristics and Password Memorability

This research revealed that several password characteristics affect password memorability. The findings here that support previous research were:

1. Password characteristics and how a password is chosen (meaningful detail, combination of meaningful details, pronounceable passwords, etc.) affect password memorability.
2. The frequency of changing a password, although it increases the level of computer-based information system security, hinders memorability,
3. The frequency of accessing an information system, which may in many cases hinder system security if the password is not changed, enhances password memorability.

Most noteworthy was the finding that password length was found not to have any effect on memorability. this can be attributed to the advent of pronounceable passwords (mnemonics) such as "2GOOD4U" and passphrases such as "I Love Paris In The Spring Time" (ILPITST) [3, 15].

Password Characteristics and Password Predictability

Results of this research show that password predictability is strongly affected by the frequency of changing a password. As previous research purports, the greater the frequency of change the greater the level of system security. Although previous research suggested that passwords made of meaningful detail, relatively short in length and simple in structure leads to predictability, the findings of this study did not support that. A notable finding that is counter to previous research is that writing down a password was not found to affect password predictability. Writing down a password violates the basic tenet of password security that holds that a password must be in the domain of something known. When a password is written down it moves into the domain of something possessed. Entities in that domain are subject to being lost, stolen or put in a place lacking security.

Password Characteristics And Sensitivity And Importance of Data Files

Although previous research revealed very little on this area of interest, this research shows that data importance and sensitivity does affect certain characteristics of user-generated passwords. Hoffman [7] suggests that the level of security should be commensurate with the importance of the resources it protects. While many users did not rate their data files as either important or sensitive, the few that did were expected

to exercise sound password security principles for password selection and use. This study showed that how a password is chosen, the number of characters in a password and password characteristics (alphabetic, alphanumeric, ASCII, etc.) were not affected by the level of data importance or sensitivity. This finding can be understood by noting that most users were asked to devise a password when they were new system users, long before they could know how important or sensitive would be their data files. It can also be noted that some users, being new to mainframe computing, likely lacked information system security consciousness.

Data importance and sensitivity were found to strongly affect where a user will work when using a computer-based information system. A security-conscious user working on sensitive or important data files will typically work in a location that is private and secure. This research also revealed that the frequency of changing a password is affected by the level of data importance and sensitivity. A security-conscious user will choose to change his or her password more frequently if they are protecting data files that are important or sensitive.

Recommendations

Recommendations for Secure Password Procedures

The following recommendations are made by Cooper [4], Morris and Thompson [14] and Pfleeger [18] to improve the level of security/access control provided by passwords:

1. Passwords should be longer.
2. Passwords should be made of meaningful detail to aid recall.
3. Passwords should contain a mix of characters such as ASCII characters.

4. Passwords should be changed frequently.

5. Passwords should not be written down.

Although passwords are widely used, confidence in their capacity to provide adequate security for computer-based information systems is decreasing.

While it is a fundamental tenet of information system security that passwords be changed frequently, almost 80% of the users surveyed in this research never changed their password. Fewer than 6% of them changed their passwords with any frequency at all. These findings prompt a need to look at the effectiveness of educational efforts to raise the security-consciousness of system users.

Recommendations for Further Research

Applications of passwords as a security mechanism have not advanced as rapidly as information technology [9, 10]. The details of password system applications and their effectiveness warrant further research.

First, the information system community enjoys a surfeit of essays and non-empirical insights into what users ought to do about password practices. This community now will benefit from channeling some of its research efforts toward investigations of what users actually do with regard to password practices.

Second, the information system would be well served if researchers in the field of system security replicated the procedures described here to challenge these findings in varying user populations and under diverse organizational conditions.

References

1. Ahituv N., Lapid Y. and Neumann S., Verifying the Authentication of an Information System User, *Computers and Security*, 6,2 (1987), 152-157.
2. Avarne S., How to Find Out a Password, *Data Processing & Communication Security*, 12,2, (Spring, 1988), 16-17.
3. Barton B.F. and Barton M.S., User-Friendly Password Methods for Computer -Mediated Information Systems, *Computers and Security*, 3,3, (1988), 186-195.
4. Cooper J.A., *Computer an Communications Security, Strategies for the 1990's*, McGraw Hill, New York, NY, 1989.
5. *Department of Defense Passwrod Management Guidline*, National Computer Security Center, CSC-STD-002-85, Washington, DC, 1985.
6. Fisher R.P., *Information Systems Security*, Prentice-Hall, Englewood Cliffs, NJ, 1984.
7. Hoffman L.J., *Modern Methods for Computer Security and Privacy*, Prentice-Hall, Englewood Cliffs, NJ, 1977.
8. Hsiao D.K., *Computer Security*, Academic Press, New York, NY, 1979.
9. Jobusch D.L. and Oldhoeft A.E., A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 1, *Computers and Security*, 8,7, (1989), 587-601.
10. Jobusch D.L. and Oldhoeft A.E., A Survey of Password Mechanisms: Weaknesses and Potential Improvements. Part 2, *Computers and Security*, 8,8, (1989), 675-689.
11. Kurzban S., A Dozen Gross 'Mythconceptions' about Information Processing, in: *Security, IFIP/sec'83*, V. Fak (editor), North Holland, pp. 15-25, 1983.
12. Landwehr C.E., The Best Available Technologies for Computer Security, *IEEE Computer*, 16,7 (July 1983), 86-99.
13. Miller G.A., The Magical Number Seven, Plus or Minus Two: Some Limits on

Our Capacity for Processing Information, *The Psychological Review*, **63**,3, (March 1956), 81-97.

14. Morris R. and Thompson K., Password Security: A Case History, *Communications of the ACM*, **22**,11, (November 1979), 594-597.

15. Menkus B., Understanding the Use of Passwords, *Computers and Security*, **7**,2, (1988), 132-136.

16. Norusis M.J., *SPSS-X Introductory Statistics Guide for Release 3*, SPSS Inc., Chicago, IL, 1988.

17. Paans R. and Herschberg I.S., Computer Security: The Long Road Ahead, *Computers and Security*, **6**,5, (1987), 403-416.

18. Pfleeger C.P., *Security in Computing*, Prentice-Hall, Englewood Cliffs, NJ, 1989.

19. Porter S.N., A Password Extension for Human Factors, *Computers and Security*, **1**,1, (1982), 54-56.

20. Siegel S. and Castellan J.N., *Nonparametric Statistics for the Behavioral Sciences*, Second Edition, McGraw Hill Inc., New York, NY., 1988.

21. Smith S.L., Authenticating Users by Word Association, *Computers and Security*, **6**,6, (1987), 464-470.

22. Spender J.C., Identifying Computer Users with Authentication Devices (Tokens), *Computers and Security*, **6**,6, (1987), 385-395.

23. Ware W.H., Information System Security and Privacy, *Communications of the ACM*, **27**,4, (April 1984), 315-321.

24. Wood C.C., Effective Information System Security with Password Controls, *Computers and Security*, **2**,1, (1983), 5-10.

25. Zviran M. and Haga W.J., Cognitive Passwords: The Key for Easy Access Control, *Computers and Security*, (1990), In press.

Appendix A

Thesis Questionnaire - Computer Password Characteristics

nproving effective information system security is a continuing problem. Passwords are widely used control access to information systems. The purpose of the questionnaire is to generate sample data the characteristics of user generated passwords at the NPS. I do not want to know your password, ly certain characteristics about it. The resulting data will be used to create a new form of passwords at are difficult to guess.

OTE:

ven if you are not a computer user or do not use the computer frequently your response to this uestionnaire will still provide us with important information.

ART A: Personal Information

Age : _____

Sex (circle one) : Male Female

Curriculum (Students) : _____
or
Department (Faculty) : _____

ART B: Password Characteristics (Please do not reveal your password !!)

Do you use the NPS mainframe system (circle one) ?

No

Yes

If no, please return this questionnaire anyway. Even if you do not use the NPS system, we appreciate completed returns to this survey.

If yes, please continue.

How many characters are in your password : _____

3. How did you choose your password (circle one)?

   A. A meaningful detail. (e.g., name, date, street)

   B. A combination of meaningful details. (e.g., Bill1989, 4june63)

   C. A pronoucable password. (e.g., one4you, 2Bfree)

   D. A random combination of characters. (e.g., carS&, dUCk*?+)

   E. Other (please specify). _____

4. What are the characteristics of your password (circle one) ?

   A. Alphabetic (e.g., abde, ERTIS) .

   B. Numeric (e.g., 1234, 5879).

   C. Alphanumeric (e.g., a34d, fo67Y1).

   D. ASCII (e.g., cd!Yx, Ac1+t6).

5. Have you ever had difficulty remembering your passwords (circle one) ?

   No

   Yes

6. Very often, computer users find it convenient to write down their password for one those unfortunate times when they forget it. Do you also practice this (circle one) ?

   Yes

   No

   If so, where do you write it down (users manual, calendar book, notebook, keyboard, on something in your wallet) ?

   where _____

7. How often did/do you change your password (circle one) ?

   A. Never
   B. Less than once a year
   C. Up to three times a year
   D. Four to six times a year
   E. About once every month
   F. More than once a month

8. Have you ever changed your password because you felt it had been guessed by someone else(circle one) ?

Yes

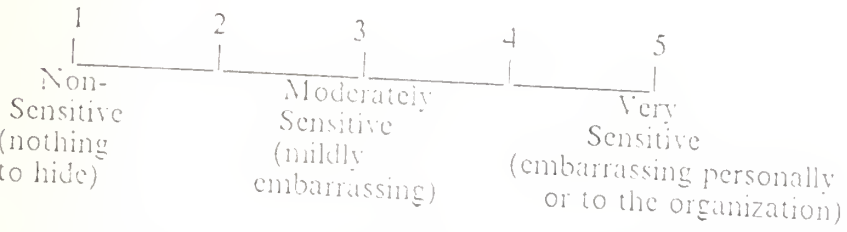
No

If so, what led you to believe it had been guessed ?

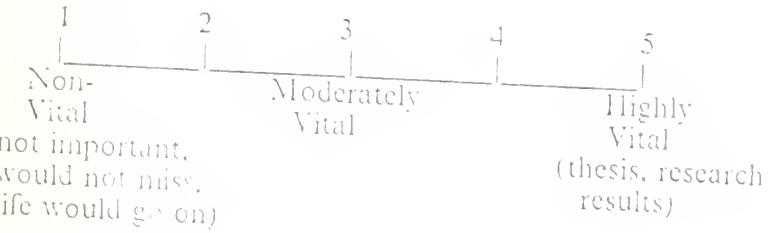
_____

_____

. On a scale of one to five, how sensitive are your data (what problems would result if revealed) (circle one) ?



. How important are your data (how vital are your data) (circle one) ?



When using a computer system, from where do you normally work (circle one) ?

A. Private office at NPS

B. Home

C. Public terminal at NPS

D. Other (please specify) _____

12. How often do you log on to the NPS mainframe (or other NPS system) (circle one)?

A. Never

B. Annually

C. Quarterly

D. At least once a month

E. Several times a month

F. At least once a week

G. Several times a week

H. At least once a day

I. Several times a day

13. Do you use any non-NPS computer systems which require the use of a password (circle one) ?

Yes

No

14. Do you use the same NPS password on non- NPS systems (circle one) ?

Yes

No

Please place completed questionnaire in the self-addressed envelope provided and return as soon as possible.

Thank you for your cooperation.

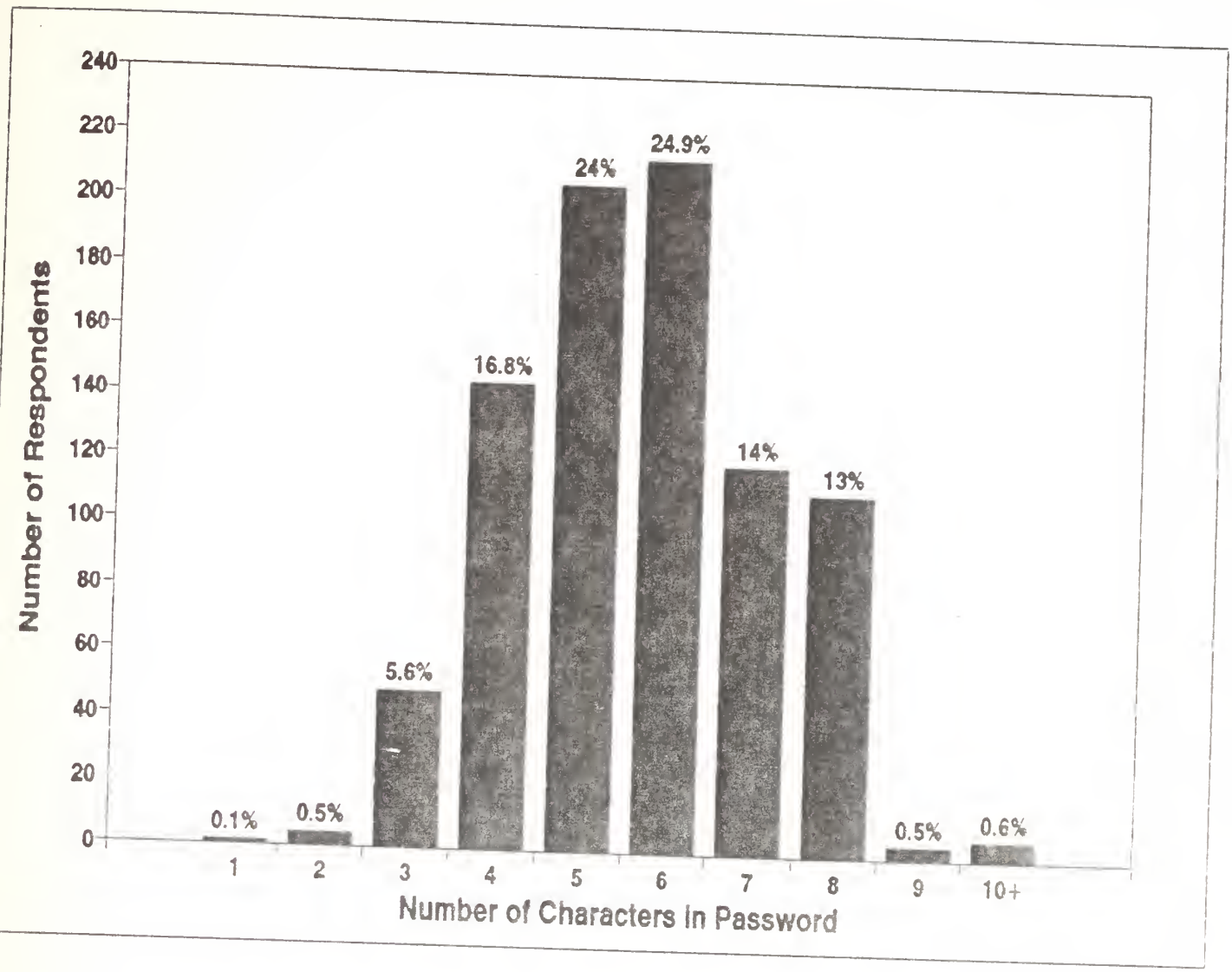


Figure 1: Number of characters in passwords

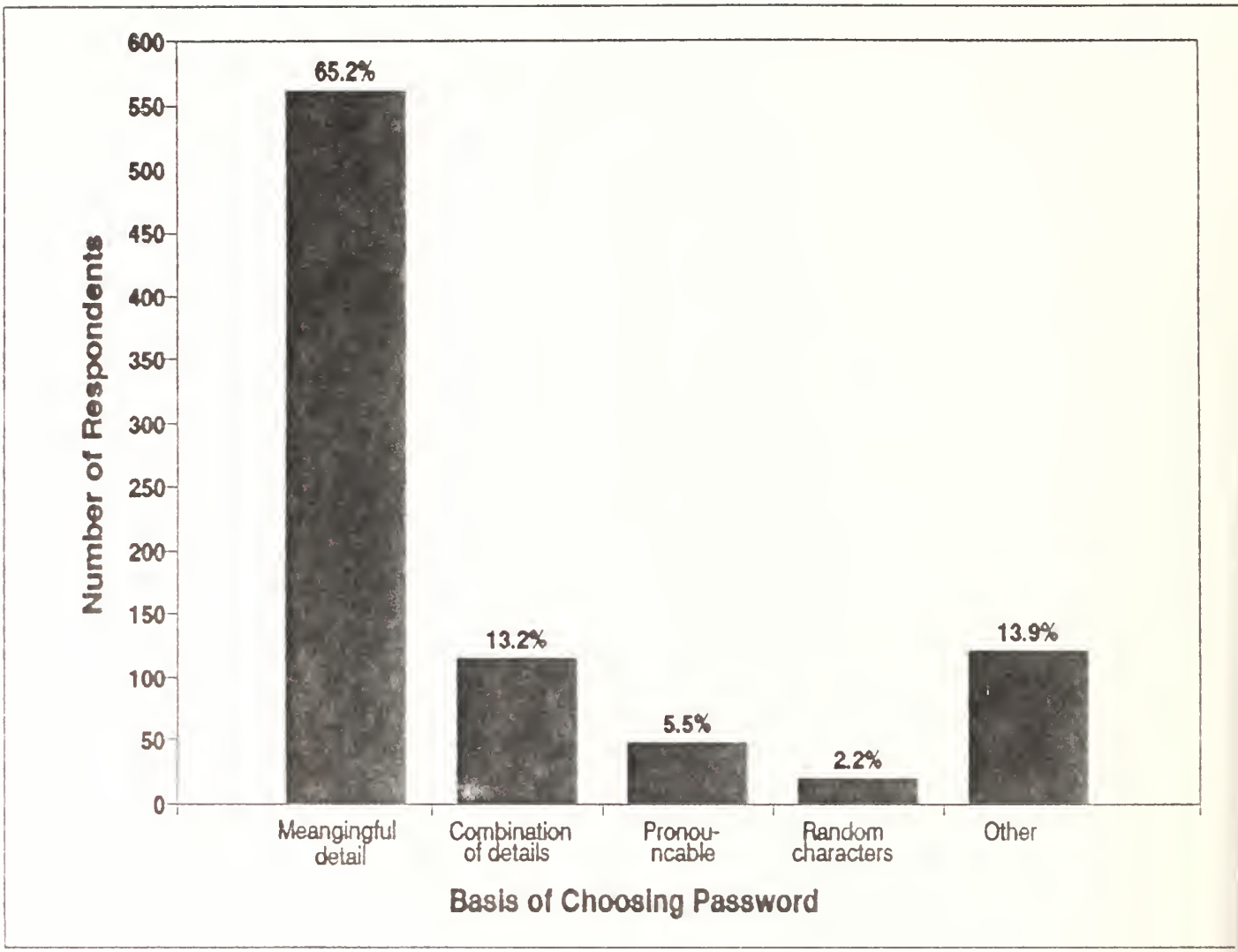


Figure 2: Basis of choosing a password

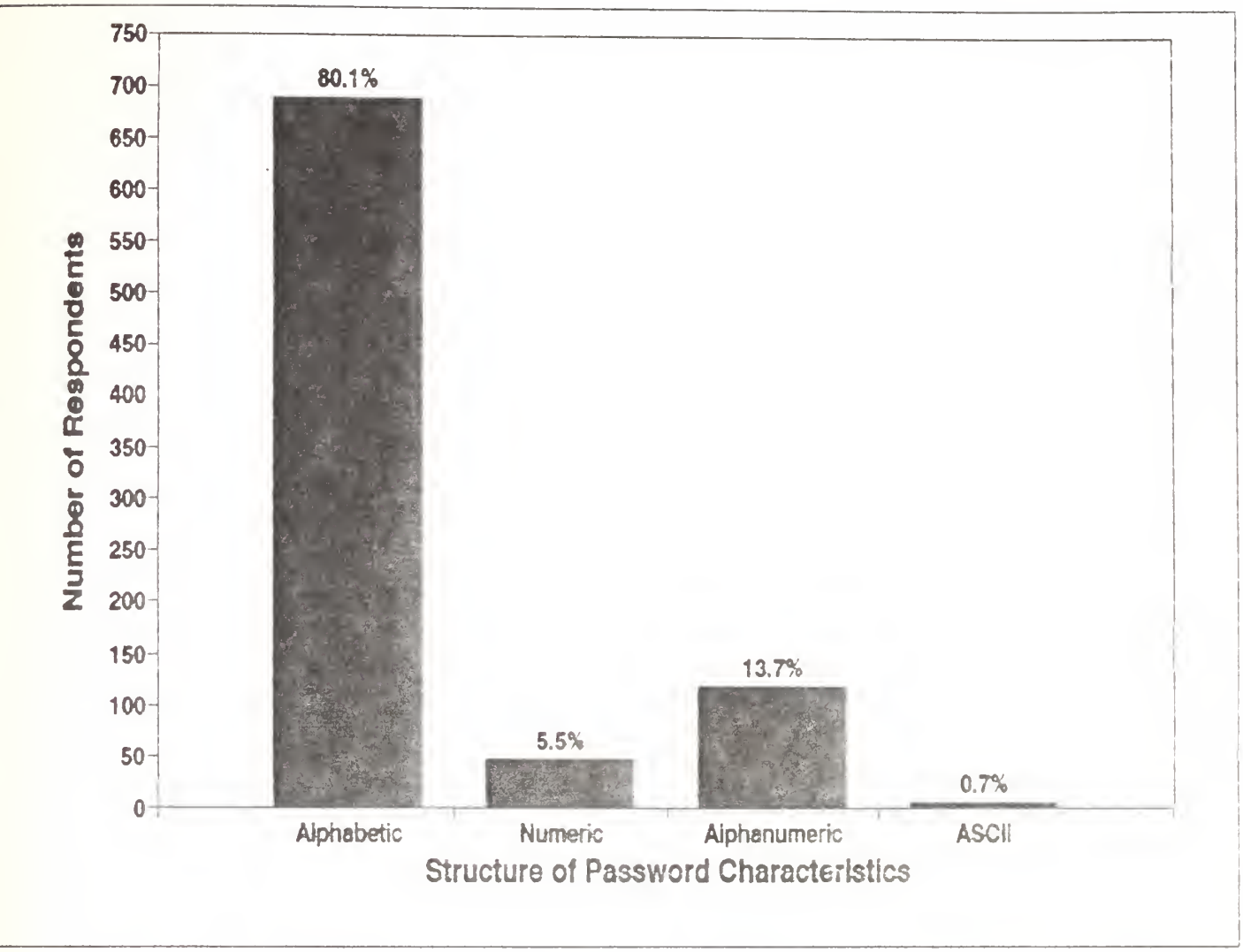


Figure 3: Structure of passwords

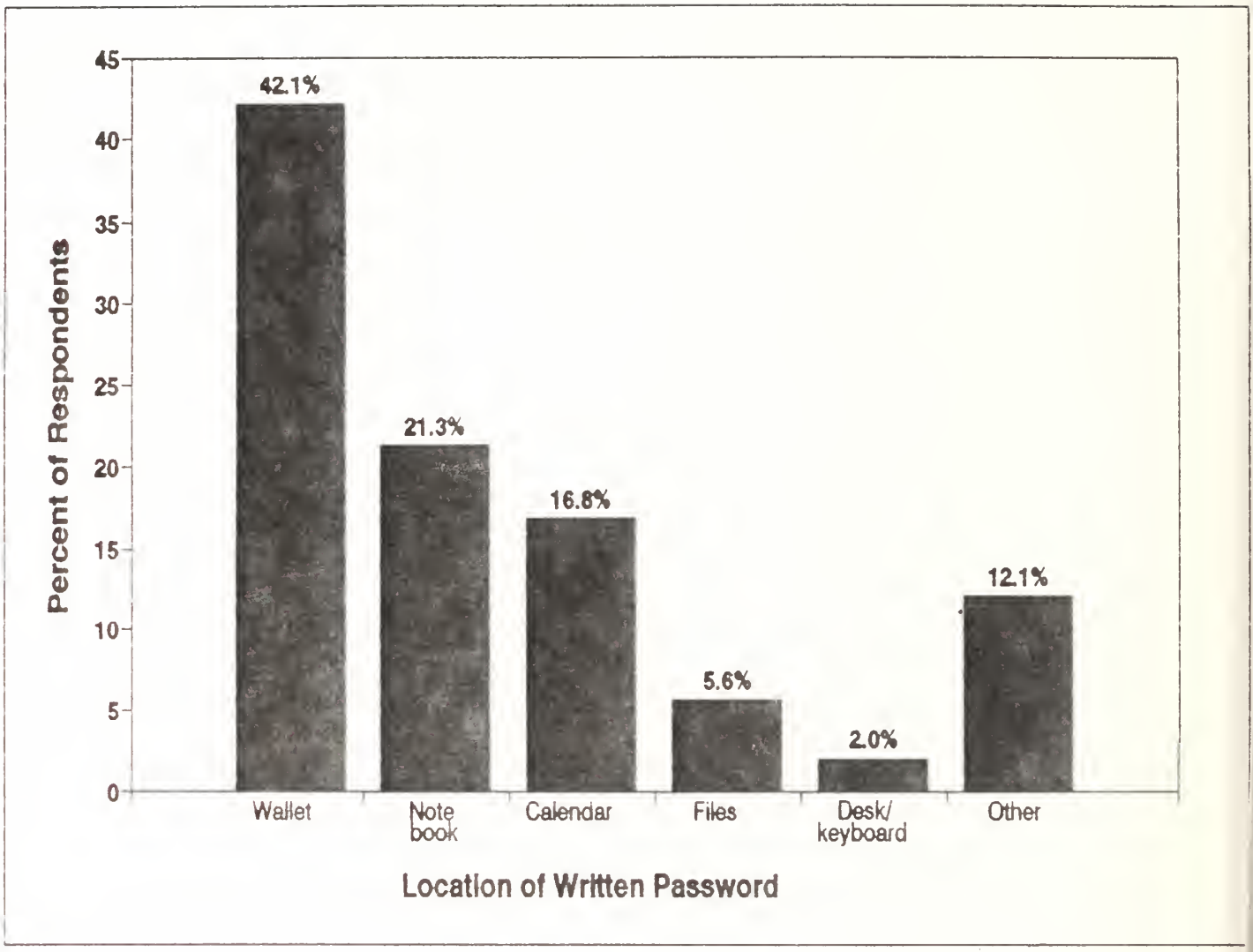


Figure 4: Location where passwords were written

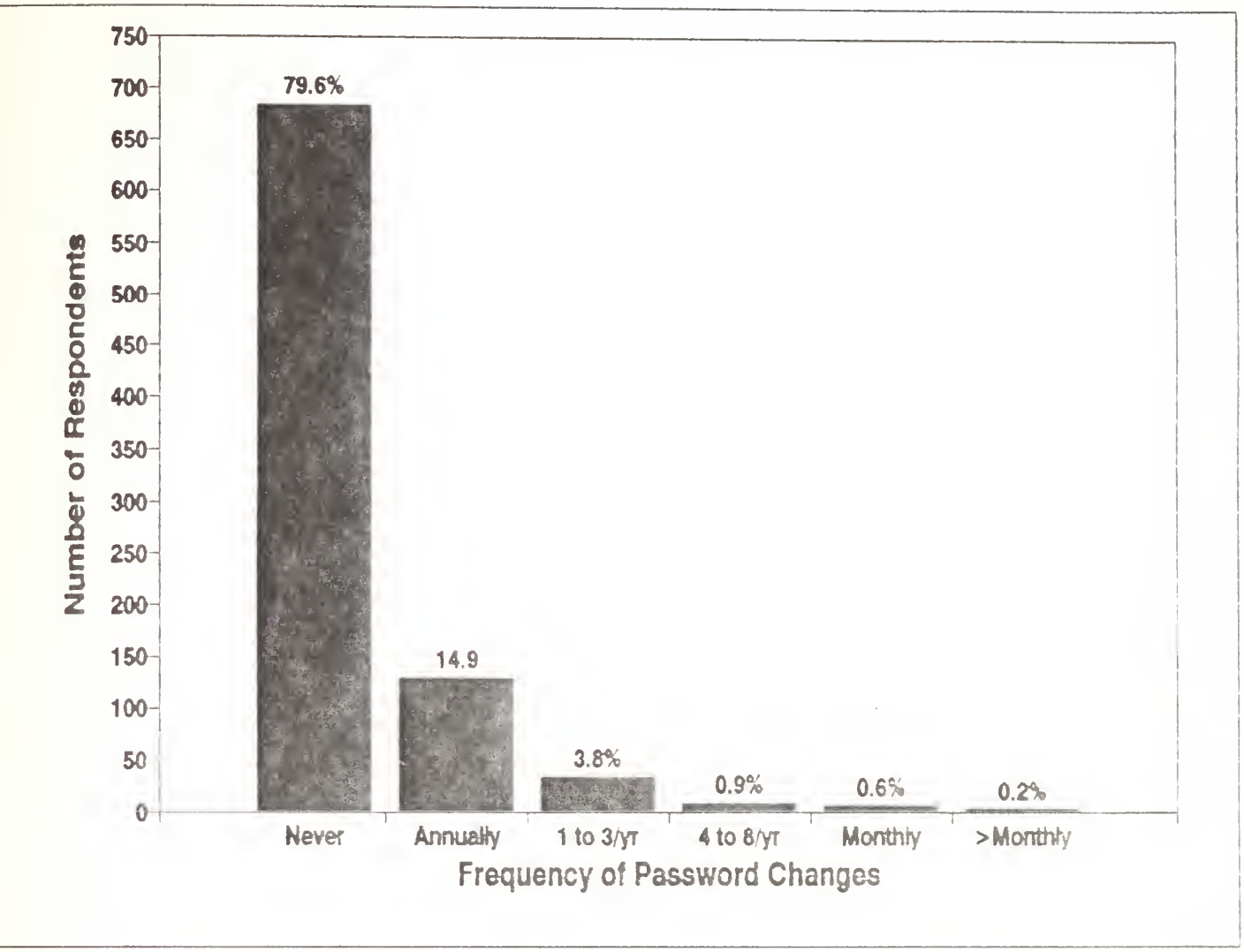


Figure 5: Frequency of changing passwords

Selection of Statistical Tests			
Data Level of Variables	**Test Used**	**Data Level of Variables**	**Test Used**
Dichotomous X Interval	T-test	Ordinal X Interval	Analysis of Variance
Dichotomous X Nominal	Cramer's V	Ordinal X Nominal	Kruskal-Wallis
Dichotomous X Ordinal	Mann-Whitney U	Ordinal X Ordinal	Spearman's Rho
Dichotomous X Dichotomous	Chi-squared		

Table 1: Selection of statistical tests

Do you write down your password?					
Variable	Level of Measure	Test	Test Value	Proba-bility	Reject Null Hypothesis
Number	Interval	T-test	-.20	.839	No
Password	Nominal	Cramer's V	.1194	.0065	Yes
Chosen	Nominal	Cramer's V	.0875	.1584	No
Change	Ordinal	Mann-Whitney	65872	.9899	No
Remember	Dichotomous	Chi-squared	38.45	.0000	Yes
Log on	Ordinal	Mann-Whitney	49783	.0000	Yes

Table 2: Association of writing down passwords with other password variables

Do you have difficulty remembering a password?					
Variable	Level of Measure	Test	Test Value	Proba-bility	Reject Null Hypothesis
Number	Interval	T-test	-.38	.706	No
Password	Nominal	Cramer's V	.1131	.0110	Yes
Chosen	Nominal	Cramer's V	.1221	.0121	Yes
Log on	Ordinal	Mann-Whitney	26259	.0214	Yes
Change	Ordinal	Mann-Whitney	25363	.0000	Yes
Same	Dichotomous	Chi-squared	1.475	.2245	No

Table 3: Association of difficulty to remember passwords with other password variables

Was your password guessed?					
Variable	Level of Measure	Test	Test Value	Proba-bility	Reject Null Hypothesis
Write	Dichotomous	Chi-squared	.5280	.4674	No
Number	Interval	T-test	-1.27	.204	No
Password	Nominal	Cramer's V	.1445	.0004	Yes
Chosen	Nominal	Cramer's V	.0935	.1145	No
Log on	Ordinal	Mann-Whitney	985.5	.4677	No
Change	Ordinal	Mann-Whitney	64125	.0000	Yes
Work	Nominal	Cramer's V	.2138	.0000	Yes

Table 4: Association of passwords predictability with other password variables

How important are your data?					
Variable	Level of Measure	Test	Test Value	Proba-bility	Reject Null Hypothesis
Write	Dichotomous	Mann-Whitney	55157	.0020	Yes
Number	Interval	ANOVA	.430	.787	No
Password	Nominal	Kruskal-Wallis	8.073	.0889	No
Chosen	Nominal	Kruskal-Wallis	12.98	.0114	Yes
Change	Ordinal	Spearman's Rho	.1916	.0000	Yes
Work	Nominal	Kruskal-Wallis	91.79	.0000	Yes

Table 5: Association of important data files with other password variables

How sensitive are your data?					
Variable	Level of Measure	Test	Test Value	Proba-bility	Reject Null Hypothesis
Write	Dichotomous	Mann-Whitney	64272	.8915	No
Number	Interval	ANOVA	1.388	.236	No
Password	Nominal	Kruskal-Wallis	2.886	.5771	No
Chosen	Nominal	Kruskal-Wallis	7.264	.1226	No
Change	Ordinal	Spearman's Rho	.1544	.0000	Yes
Work	Nominal	Kruskal-Wallis	29.13	.0000	Yes

Table 6: Association of sensitive data files with other password variables

Distribution List

Agency	No. of copies
Defense Technical Information Center Cameron Station Alexandria, VA 22314	2
Dudley Knox Library, Code 0142 Naval Postgraduate School Monterey, CA 93943	2
Office of Research Administration Code 012A Naval Postgraduate School Monterey, CA 93943	1
Library, Center for Naval Analyses 4401 Ford Avenue Alexandria, VA 22302-0268	1
Department of Administrative Sciences Code AS Naval Postgraduate School Monterey, CA 93943	1
Professor Moshe Zviran, Code AS/Zv Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943	6
Professor William J. Haga, Code AS/Hg Department of Administrative Sciences Naval Postgraduate School Monterey, CA 93943	6
LtC. Rayford B. Vaughn, Code C11 National Computer Security Center 9800 Savage Road Fort Meade, Maryland 20755-6000	2